Monthly Security Tips Newsletter
February 2009

CISO Tips

Remember to protect your home computer from access to unsafe and undesirable sites. Try Blue Coat's™ free home offering at http://www1.k9webprotection.com/;

Pay particular attention to obtaining a top line anti-virus and anti-spyware program (e.g., Symantec, Trend Micro, Norton Utilities) to block & eradicate malware; such as, key-loggers and hidden malware. Educate your family members and other friends that are new to the dangers of not properly protecting their new computers and networks. Please see Recognizing and Avoiding Spyware: www.msisac.org/awareness/news/2007-06.cfm

To view State security policies, please visit: http://isd.alabama.gov/policies/policies.aspx?sm=c_a; or visit: http://isd.alabama.gov/default.aspx to view other Policies/Security dropdown links.

*ALERT: please see "**REVISED!**" security documents Standard 640-02S2

Cyber Security Trends for 2009

The volume and complexity of cyber threats continue to increase. More of our activities—whether at home, school or work—involve computers and the Internet—in fact, in the not-too-distant future, your household appliances may be computerized and controlled remotely from your PDAs; simultaneously, the knowledge required to launch a successful attack continues to decrease. As we develop more defenses, the cyber criminals and hackers come up with new ways to attack our computers. These factors create an environment in which vigilance on a daily basis is required to help mitigate the risks. Threats such as identity theft, worms and viruses, loss of sensitive information and other malicious activity are part of an ever-evolving cyber security threat landscape.

Some of the key challenges we are facing in 2009 focus on application security. Application security is a crucial layer in a multi-tiered cyber security strategy. Building security in at the beginning of development is an important factor in minimizing potential vulnerabilities. We've seen the results when vulnerabilities in web applications are exploited, leading to SQL injection attacks, cross-site scripting and other malicious activity.

Cyber criminals take advantage of commercial web sites that have poor security to add code to the web site without the knowledge of the web hosting company. That code may silently re-direct the user's computer to another site which will download malware to the user's computer, without the user's knowledge; the attackers may also add a script to the site that will automatically execute on the user's computer.

Another alarming trend continues to be the evolution of cyber crime, which has morphed from fairly innocuous web-site hacking and "graffiti" attacks to organized crime syndicates seeking profit. Cyber crime is now big business. Attackers now want your credit card and other financial information as well as your social security number. According to a recent study by McAfee, the global cost of cyber crime due to identity theft and data breaches is an estimated one trillion dollars. Many data thefts are orchestrated by organized crime, both in the U.S. and abroad.

The economic recession is another factor that may impact cyber security challenges. The risks due to insider threats are another major concern, and are expected to increase due to the economic downturn. Additionally, phishing scams and other social engineering attacks will increase, as attackers try to take advantage of bank closings, claims for "easy credit" or other online scams. Phishing attempts are no longer easily detected based on misspelled words in the email scam, or claims of large sums of money left to you in some foreign location, for example. The phishing scams are becoming more targeted and more "realistic" in appearance.

Holidays and major news events are still popular vehicles for compromising computers. Valentine's Day is this month and email messages are already circulating that will infect a user's computer when the message is clicked. Once the computer is infected, the malware will attempt to capture the user's personal information and transmit it to the cyber criminals.

What can be done to make to protect my computer and my personal information?

Good security is implemented through a multi-layer approach. Users can minimize risk by following the recommendations below:

- Install and maintain a firewall.
- Use anti-virus and anti-spyware software and set them to auto-update.
- Keep operating system and other software up-to-date by enabling the auto-update feature.
- Be cautious about all communications; think before you click. If an email appears to be a phishing communication, do not respond. Delete it.
- Do not open email or related attachments from untrusted sources.

If you receive an email appearing to be from a legitimate business, requesting the submission of personal information, it is most likely a scam. Legitimate businesses do not send emails requesting personal information.

For additional information on Challenge or Secret Questions, please visit:

- Phishing: How to Avoid Getting Hooked: **www.msisac.org/awareness/news/2008-10.cfm**
- Web Browser Attacks: **www.msisac.org/awareness/news/2008-10.cfm**
- Online Shopping: **www.msisac.org/awareness/news/2007-12.cfm**
- Top Ten Cyber Security Tips: **www.msisac.org/awareness/news/2006-10.cfm**

For more monthly cyber security newsletter tips visit: www.msisac.org/awareness/news/

The information provided in the Monthly Security Tips Newsletters is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture.

MS-ISAC

www.msiac.org